a storage element that stores an encryption of a security key, the encryption being based on a second biometric key of an authorized user,

a biometric decrypter, operably coupled to the biometric sensor and the storage element, that decrypts the encryption of the security key, producing thereby a decrypted security key that is equal to the security key when the first biometric key is equivalent to the second biometric key, and

an authentication encrypter, operably coupled to the biometric decrypter, that encrypts a challenge parameter to produce a response parameter that is based upon the decrypted security key.

2. (CANCELED)

3. (AMENDED) The security token of claim 1, further including:

a token identifier that provides an identification that is associated with the authorized user.

4. The security token of claim 1, further including:

a token identifier that provides an identification that is associated with the authorized user.

5. The security token of claim 1, wherein

the biometric sensor provides the first biometric key based upon a hash of the biometric measure of the current user.

6. The security token of claim 1, wherein

the second biometric key is a symmetric key.

7. (AMENDED) The security token of claim 1, wherein

the security key is a private key of a set of asymmetric keys that include at least one private key and at least one public key.

8. (AMENDED) The security token of claim 1, further including

a one-time encrypter that produces the encryption of the security key based upon the second biometric key.

Sub C2

9. (AMENDED) A security system comprising:

a token that includes:

a biometric sensor that provides a first biometric key of a current user of the token based upon a biometric measure of the current user,

an encryption of a security key, the encryption being based upon a second biometric key of an authorized user, and

a biometric decrypter that decrypts the encryption of the security key to produce a decrypted security key, such that

the decrypted security key is equivalent to the security key when the first biometric key is equivalent to the second biometric key,

the decrypted security key is an erroneous key when the first biometric key is different from the second biometric key; and

an authentication encrypter, operably coupled to the biometric decrypter, that encrypts a challenge parameter to produce a response parameter that is based upon the decrypted security key; and

an access device that, when operably coupled to the token, determines an access status based upon the decrypted security key.

10. The security system of claim 9, wherein

the access status is a verification that the current user is the authorized user.

11. The security system of claim 9, wherein the access device includes:

a challenge device that provides a challenge parameter to the token, and

a receiving device that receives a response parameter from the token based upon the challenge parameter and the decrypted security key;

wherein the access status is based upon the response parameter.

12. (CANCELED)

13. (AMENDED) The security system of claim 11, wherein:

the security key is a first key of a pair of asymmetric keys, and

the receiving device includes:

an authentication decrypter that decrypts the response parameter to produce a decrypted result, the decryption being based upon a second key of the pair of asymmetric keys, and

a comparator that compares the decrypted result with the challenge parameters to determine the access status.

14. The security system of claim 13, further including:

a database of authorized user keys from which the second key of the pair of asymmetric keys corresponding to the authorized user is determine.

13

15. The security system of claim 14, wherein:

the token further includes a token identifier that provides an identification corresponding to the authorized user, and

the determination of the second key of the pair of asymmetric keys from the database of authorized user keys is based upon the identification corresponding to the authorized user.

16. (AMENDED) The security system of claim 11, wherein the token further includes:

an encapsulation that obstructs access to components of the token, and

a means for destroying at least one of the second biometric key and the encryption of the security key when the encapsulation is breached.

17. The security system of claim 11, wherein the access device further includes:

a random number generator to facilitate the determination of the access status based upon the decrypted security key.

18. (AMENDED) A method for determining an access status comprising the steps of:

encrypting a security key to produce an encrypted security key based upon a first biometric key of an authorized user into a token,

determining a second biometric key of a current user of the token based upon a biometric measure of the current user,

decrypting the encrypted security key to produce a decrypted security key based upon the second biometric measure, and

determining an access status based upon the decrypted security key.

19. The method of claim 18, further including the steps of:

communicating a challenge parameter to the token, and

determining a response parameter based upon the challenge parameter and the second biometric key; and

wherein the step of determining the access status is based upon the response parameter.

20. (AMENDED) The method of claim 19, wherein

the security key is a first key of a pair of asymmetric keys,

the step of determining the response parameter includes the step of encrypting the challenge parameter based upon the second biometric key, and

the step of determining the access status includes the steps of:

decrypting the response parameter to produce a decrypted result based upon a second key of the pair of asymmetric keys, and

comparing the decrypted result to the challenge parameter to determine the access status.

REMARKS

Claims 2 and 12 have been canceled, without prejudice or disclaimer. Claims 1, 3-11, and 13-20 are pending of which Claims 1, 3, 7-9, 13, 16, 18, and 20 have been amended. Applicant has carefully considered the application in view of the Examiner's action and, in light